

Livre blanc

Correctifs logiciels : la « ceinture de cybersécurité »

16 septembre 2021





About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

De nos jours, tous les véhicules sont équipés de ceintures de sécurité. Logique, puisque les études montrent clairement que ces dispositifs sauvent des vies et atténuent le risque de blessures. L'agence fédérale américaine des Centres pour le contrôle et la prévention des maladies (CDC) estime par exemple que « les ceintures de sécurité réduisent environ de moitié les séquelles graves et les décès liés aux accidents de la route ».

Ce chiffre est d'autant plus parlant quand on sait qu'aux États-Unis, toujours d'après les CDC, « les services d'urgence ont accueilli plus de 2,2 millions de conducteurs et de passagers adultes impliqués dans un accident de la circulation en 2012 » et que, la même année, « les blessures dues à des collisions non mortelles ont entraîné plus de 50 milliards de dollars de frais imputables aux soins médicaux à vie et à la perte d'emploi ».

Pourtant, chaque année, trop de personnes perdent encore la vie ou gardent de lourdes séquelles parce qu'elles n'ont pas attaché leur ceinture de sécurité.

Imaginez le nombre de victimes si cet équipement n'était pas obligatoire à bord de nos véhicules. Chaque conducteur, engageant sa propre responsabilité, devrait rechercher et comparer les options disponibles, acheter le dispositif de son choix, l'installer, veiller à son efficacité et s'occuper de sa maintenance.



Dans ce scénario, croyez-vous que la majeure partie des automobilistes ferait l'impasse sur cet investissement de sécurité ? Cela est peu probable, étant donné que nous connaissons tous les risques auxquels nous nous exposons en conduisant sans ceinture.

Mais pour des raisons qui semblent défier la logique, bon nombre d'entreprises refusent toujours d'investir dans des solutions de gestion et d'automatisation des correctifs. Certains dirigeants pensent en effet qu'il est plus simple et plus rentable pour leurs équipes de travailler sur des systèmes mal voire non sécurisés. Ils connaissent pourtant l'ampleur des risques encourus et voient d'autres entreprises du secteur payer régulièrement, chèrement et publiquement cette négligence.



Les correctifs : un rempart précieux mais négligé

Dans le domaine de la sécurité informatique, on ne soulignera jamais assez l'importance d'une gestion proactive des correctifs et des outils associés. L'Australian Signals Directorate, le service de renseignement australien responsable des questions de sécurité de l'information, estime qu'au moins 85 % des cyberattaques ciblées peuvent être évitées en suivant ces quatre étapes simples :

- Établir une liste blanche des applications
- Corriger les applications
- Corriger les systèmes d'exploitation
- Restreindre les droits d'administrateur

Tous les experts en sécurité vous le diront : la gestion des mises à jour correctives est un élément essentiel d'une bonne stratégie de défense. En juillet 2015, Google a publié une étude interrogeant 231 professionnels de la cybersécurité et 294 internautes « lambda » sur la façon dont ils protègent leurs données sensibles. L'installation des mises à jour logicielles est la première mesure de protection citée par les experts, avant l'utilisation de mots de passe renforcés et l'authentification à deux facteurs. Près de 35 % des experts estiment que les mises à jour logicielles sont importantes, contre seulement 2 % des internautes non-initiés, qui privilégient quant à eux les antivirus et les mots de passe.

Bien souvent, une gestion efficace des correctifs est non seulement précieuse mais aussi essentielle pour les entreprises. Comme le souligne HP dans son rapport de juin 2015 intitulé *The Hidden Dangers of Inadequate Patching,* « la conformité aux normes sectorielles ainsi qu'aux réglementations gouvernementales requiert une stratégie renforcée de maintenance et d'application des correctifs ». La norme PCI DSS (Payment Card Industry Data Security Standard) et la directive européenne NIS (Network and Information Security) sont deux exemples de réglementations imposant une telle stratégie.

Pourtant, malgré son importance évidente, la gestion des correctifs reste un problème largement non résolu. Selon le rapport d'enquête 2015 sur les violations de données publié par Verizon (DBIR), « 99,9 % des vulnérabilités exploitées ont été compromises plus d'un an après leur inscription au dictionnaire des failles et vulnérabilités communes (CVE). » Encore plus troublant, le document indique que « beaucoup de vulnérabilités persistent principalement parce que les correctifs de sécurité nécessaires n'ont jamais été implémentés. En effet, la plupart d'entre elles ont été observées pour la première fois en 2007 et remontent donc à plus de huit ans. »

85% des cyberattaques ciblées peuvent être évitées en suivant ces quatre étapes simples :

1. Établir une liste blanche des applications
2. Corriger les applications
3. Corriger les systèmes d'exploitation
4. Restreindre les droits d'administrateur

*Australian Signals Directorate



Dans un communiqué d'avril 2015, l'US-CERT (un service du département de la Sécurité intérieure des États-Unis) répertorie les « 30 vulnérabilités à haut risque les plus ciblées ». On y apprend que les bulletins de sécurité ou références CVE les plus anciens au sujet de ces 30 vulnérabilités remontent à 2006.

Comment améliorer la gestion des correctifs ?

Comme le dit si bien Google dans l'étude mentionnée plus haut, « Les mises à jour logicielles [...] sont votre ceinture de sécurité en ligne et assurent votre protection. Pourtant, bon nombre d'internautes négligent cette bonne pratique, jugeant même qu'elle est susceptible de poser un risque de sécurité. »

À tort ou à raison, c'est une inquiétude que partagent également certains experts. L'étude HP met en évidence les arguments qu'avancent des entreprises (pourtant soucieuses de leur sécurité) pour expliquer leur méfiance à l'égard des correctifs.

- Les correctifs font planter les systèmes
- Les correctifs introduisent des problèmes de sécurité
- Les correctifs ne fonctionnent jamais comme prévu
- Les correctifs sont livrés avec des « fonctions bonus » non communiquées et non souhaitées
- Les déploiements de correctifs « silencieux » perturbent les utilisateurs ou la résolution des problèmes

D'autre part, la détection et la hiérarchisation des systèmes à corriger n'est pas une mince affaire, et les choses se compliquent d'autant plus lorsqu'il faut prendre en compte les utilisateurs mobiles, distants ou itinérants.

Fort heureusement, les solutions modernes permettent de répondre à ces inquiétudes. Par exemple, les correctifs rigoureusement testés et inspectés avant d'être distribués aux entreprises ont peu de chances de faire planter vos systèmes, d'introduire des problèmes de sécurité, de ne pas fonctionner comme prévu ou d'inclure des fonctionnalités indésirables. Aussi, les paramètres de ces plateformes vous permettent de distribuer les correctifs sans perturber les utilisateurs ni votre activité. Enfin, les solutions modernes déploient et gèrent les mises à jour correctives pour l'ensemble des systèmes d'exploitation et des applications tierces critiques de votre entreprise.

Les entreprises souhaitant sécuriser des environnements plus larges et complexes ont tout intérêt à adopter une méthodologie spécifique afin de hiérarchiser les priorités. Le développement et l'exécution de cette approche doivent s'appuyer sur des exigences et des objectifs métier spécifiques. Pour autant, il n'est pas nécessaire de partir d'une toile vierge. Forrester Research, par exemple, propose à ses clients sa solution P3 (Prioritized Patching Process) dédiée.

Dans sa newsletter de février 2014, ISACA, une association professionnelle IT à but non lucratif, résume ce processus en « Quatre étapes essentielles au processus de gestion des correctifs » :

1. Estimez votre niveau de sécurité par le biais d'une modélisation prédictive des menaces afin d'identifier les ressources les plus vulnérables et de déterminer leur risque de compromission.



2. Mesurez les effets d'un exploit potentiel en vous basant sur le type et la sensibilité des données stockées et consultées par chacune de ces ressources.
3. Mesurez le « risque intrinsèque » de chaque vulnérabilité, en vous appuyant sur plusieurs facteurs (par exemple, si cette vulnérabilité a déjà été exploitée par le passé, et le degré de malveillance de cet exploit).
4. Priorisez les mises à jour correctives en fonction des trois critères précédents.

Ces opérations, bien qu'essentielles à la mise en œuvre d'une gestion efficace des correctifs, ne sont qu'une partie du processus. L'étude de HP identifie les autres étapes nécessaires.

1. Détection complète et précise de toutes les ressources
2. Identification des ressources à protéger et des processus requis à cette fin
3. Identification de fournisseurs fiables et échanges constants avec ces derniers (via un abonnement à leurs listes d'e-mailing ou réseaux sociaux)
4. Détermination de la meilleure façon d'installer et de gérer les correctifs requis, en s'appuyant sur différents facteurs tels que le coût du recrutement ou de solutions automatisées, les taux de défaillance des correctifs et les délais de déploiement

Vous pouvez consulter les ressources de cabinets d'étude, de fournisseurs de solutions de gestion des correctifs et de leurs partenaires d'intégration afin d'obtenir d'autres conseils stratégiques en matière de hiérarchisation et d'exécution. Toutefois, sachez qu'il est possible d'améliorer votre gestion des correctifs sans nécessairement passer par ces interlocuteurs. Pour commencer, vous devrez renforcer votre stratégie d'identification, d'évaluation, de déploiement et de gestion des correctifs pour vos systèmes et applications les plus critiques.

Vous pouvez consulter les ressources de cabinets d'étude, de fournisseurs de solutions de gestion des correctifs et de leurs partenaires d'intégration afin d'obtenir d'autres conseils stratégiques en matière de hiérarchisation et d'exécution. Toutefois, sachez qu'il est possible d'améliorer votre gestion des correctifs sans nécessairement passer par ces interlocuteurs. Pour commencer, vous devrez renforcer votre stratégie d'identification, d'évaluation, de déploiement et de gestion des correctifs pour vos systèmes et applications les plus critiques.

Une administration IT efficace requiert des ressources, systèmes et services entièrement et parfaitement sécurisés. Or, une sécurité exhaustive, efficace et centrée sur les utilisateurs nécessite avant tout une gestion des correctifs à la fois pertinente et complète.

Une administration IT efficace requiert des ressources, systèmes et services entièrement et parfaitement sécurisés. Or, une sécurité exhaustive, efficace et centrée sur les utilisateurs nécessite avant tout une gestion des correctifs à la fois pertinente et complète.



Avantages d'Avast Business

Dans une voiture, la ceinture de sécurité nous protège tout en nous laissant une certaine liberté de mouvement pour atteindre ce dont nous avons besoin. Avast Business propose tous les outils et services nécessaires pour mettre en œuvre une gestion des correctifs complète, consolidée et automatisée à l'échelle de votre entreprise.

Nos produits offrent une protection multi-niveaux pour défendre vos utilisateurs et vos ressources informatiques contre les menaces les plus sophistiquées. Notre portefeuille comprend des antivirus nouvelle génération, des outils de test, déploiement et gestion automatisés des correctifs pour systèmes Microsoft Windows et applications tierces, la sauvegarde dans le cloud, des passerelles web sécurisées, un accès réseau Zero Trust et bien plus encore.

Nos solutions sont intégrées au sein d'une seule et même plateforme sécurisée, ce qui permet l'automatisation rapide des politiques d'administration et de sécurité informatique, tout en offrant une visibilité inégalée sur les activités de gestion et de protection de votre environnement informatique.

La plateforme de sécurité d'Avast Business propose également des rapports et des tableaux de bord complets et personnalisables. Ils vous permettent d'affiner votre visibilité sur les risques et les menaces, de veiller à la conformité réglementaire et politique, et d'améliorer votre niveau de sécurité général. Pour plus d'informations, contactez votre responsable commercial Avast Business ou rendez-vous sur la page des solutions **avast.com/business.**